Authentication and security

Individuals who are granted access to the computing and storage resources that CISL manages use their assigned user names and one of the authentication methods that are described below to log in to those systems.

Passwords, apps, tokens, and PINs must be protected and may not be shared with anyone. If sharing is detected, CISL will disable the accounts of those involved. The same applies to passwords that give users access to internal UCAR systems.

UCAR and NCAR computers, computing systems, and associated communications systems are to be used for official business only. By signing the required authentication acknowledgement form, you agree not to misuse these resources, and you accept responsibility for activity associated with your username and token. You also agree not to duplicate or use copyrighted or proprietary software without proper authorization.

Page contents

Duo two-factor authentication

Logging in with the Duo two-factor authentication (2FA) service requires the user to enter a "CIT" password in conjunction with the **Duo Mobile** app or a landline phone. See Authenticating with Duo for details.

Using tokens

Some users log in with a **YubiKey 4** authentication token and CIT password.

See the YubiKey web page for how to use the token.

Returning your YubiKey 4 token

You must return your YubiKey 4 token when your project ends or when you will no longer be using NCAR/CISL computing and storage resources. Place it in a protective envelope and include a note with your name, username, and reason for returning the token.

CISL charges a fee for lost or unreturned YubiKey 4 tokens.

Return your authentication token to:

> **UCAR Shipping and Receiving**
> **c/o Research Computing Help Desk - Mesa Lab**
> **3090 Center Green Drive**
> **Boulder, CO 80301**

Token pick-up, drop-off at the Mesa Lab

Call 303-497-2400 to make arrangements.

Security overview

All users must comply with UCAR computer security policies and procedures. See Access to and Use of Information Systems and Technology Infrastructure (staff login required).

We strive to maximize the availability and value of our computer and network systems by protecting them from unauthorized access. Good security practices help prevent data loss or corruption, malicious activity, and loss of computer time.

As a user, you have an important role in ensuring the security of these resources. In addition to protecting the passwords, PINS, and tokens that give you access to our systems, we ask that you do the following:

Loss, theft, or compromise

Loss, theft, or compromise of a YubiKey must be reported within 48 hours to the Research Computing Help Desk at x2400 (303-497-2400). Quick reporting will help the organization minimize security risk.

Protecting your Duo app or YubiKey token

You must protect your Duo or YubiKey solution by agreeing to the following:

- Your YubiKey token or Duo application will remain in your custody and is for your use only; it may not be shared.
- You will immediately (within 48 hours) report loss of custody of your hardware authentication token to the Research Computing Help Desk at x2400 (303-497-2400). Loss of custody may be due to loss or theft.
- Your PIN number or CIT password may not be shared or made available in unencrypted electronic form.
- Compromise (disclosure of PIN number or CIT password) must be reported to the Research Computing Help Desk at x2400 (303-497-2400) and /or to the UCAR Security Operations Center at x4300 (307-996-4300).

Protect your PIN

Do not leave your PIN where others may view it, and do not affix it to your workstation or your token. Do not use the same PIN that you use for debit cards or credit cards.

Try to memorize your PIN instead of writing it down. You may write it down, but do not store it with the token. If you do write it down, keep it where others cannot access it, such as in a locked desk drawer or file cabinet that only you can access.

Use encryption for logging in and transferring files

Our systems require this, but it also is good practice to use encryption for other computers and systems.

Patch your systems and use anti-virus software

This applies to any computer from which you log in to UCAR and NCAR systems. If you are using your own personal computer or another non-UCAR or non-NCAR computer, be sure that it is kept up to date with the latest software patches and anti-virus protection.

If you are planning to visit UCAR and bringing your own computer, discuss wireless and guest network access with your UCAR contact before you arrive. Procedures regarding guest network access also apply to personally owned computers that UCAR and NCAR staff bring in.

Be careful

Be aware of email scams and so-called "social engineering" methods that hackers and fraudsters use to gain access to passwords and other information. Never give anyone your password. UCAR and NCAR system administrators will not ask you for your password via phone or email.

Other cautions

- Don't run strange binaries or executables.
- Don't log in to sites that you receive in email or other messages, especially if the message seems urgent and you are not familiar with the site.
- Some malware is spread via USB flash drives, so make sure any flash drives that you use are from trusted sources.